## ABSTRACT

A client-forced authentication mechanism for network communication enables a client to choose to "force" the establishment of an authenticated connection with a server

5 that supports both authenticated and non-authenticated connections, while allowing the client to communicate with older servers that do not support client-forced authentication. To establish an authenticated connection with a server, the client includes authentication request data in a

10 communication packet to the server. The authentication request data are designed such that a server supporting forced authentication would recognize them and give a predefined response, while an older server that does not recognize such data would respond with a well-defined error message according

15 to the underlying network communication protocols. The exact format, location, and contents of the authentication request data depend on the underlying communication protocols and may be implemented in various ways. Based on the response from the server, the client is able to tell whether the server

20 supports client-forced authentication. If so, the client sends its credentials to the server for authentication. If not, the client may determine whether to communicate with the server over a non-authenticated connection.